

Forum: [Hack Forums](#)

Thread: [Dumping RDP creds on Windows machine](#)

Noctem187 - July 17, 2023, 7:35 am

How would I dump saved RDP creds once I have access to a machine?

I have tried dumping lssas service and have located the file but i don't get much.

Sage - July 17, 2023, 7:37 am

My software in my signature grab the RDP creds saved on windows machine

Mr. Robot - July 18, 2023, 5:28 am

(Jul 17, 2023 07:37 AM)Sage Wrote: [\[CITE\]](#) My software in my signature grab the RDP creds saved on windows machine

<https://gridinsoft.com/blogs/wise-remote-trojan-infostealer-rat-ddos-bot-and-ransomware/>

<https://www.cyfirma.com/outofband/wise-remote-stealer-unleashed-unveiling-its-multifaceted-malicious-arsenal/>

DramaKing - July 18, 2023, 6:22 am

There are credential stealers, but here's how you would do it. Saved RDP credentials are stored with Credential Manager (credman) in %localappdata%\Microsoft\Credentials using CryptProtectData (DPAPI).

Noctem187 - July 18, 2023, 6:57 am

(Jul 18, 2023 06:22 AM)DramaKing Wrote: [\[CITE\]](#) There are credential stealers, but here's how you would do it. Saved RDP credentials are stored with Credential Manager (credman) in %localappdata%\Microsoft\Credentials using CryptProtectData (DPAPI).

Thank you, ill try this out.

I was looking for something not requiring tools, just the location then I can run it through hashcat.

DramaKing - July 18, 2023, 8:18 am

Hashcat is a tool, and though DPAPI is not a hashing algorithm, it looks like you can use modes 15300, 15310, 15900, and 15910 that were included in builds later than 3/2022.